A. POLICIES AND PROCEDURES				
Objective: to provide management direction and support for security in accordance with business requirements and relevant laws and regulations.				
No.	**Type**	**Control**	**Description**	**Considerations**
A.1.	**Active**	**Identification of applicable legislation and contractual requirements**	All relevant legislative, statutory, regulatory and contractual requirements, and the organisation's approach to meet these requirements, shall be explicitly identified, documented and kept up to date for all security policies and prepare and response related procedures.	Consider: • Health and Safety at Work Act 1974 • Management of Health & Safety at Work Regulations 1992 (updated 1999)
A.2.	**Active**	**Security, preparedness and response policies**	The organisation shall determine the scope, requirements, and management responsibilities for security management (including preparedness and response). This should be captured in a policy (or set of policies) that shall be defined and approved by management, and published and communicated to employees and any relevant external parties.	Consider: • Scope • Objectives • Legal & regulatory obligations • Responsibilities • Related policies (e.g. access control, cyber security etc.)
A.3.	**Active**	**Review of security, preparedness and response policies**	Policies and management responsibilities in relation to security, including preparedness and response, shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Consider: • Annual review / periodic review • Review following: change to threat landscape, increase in vulnerabilities, resourcing, or assets
A.4.	**Active**	**Security, preparedness and response related procedures and plans**	A set of procedures and plans in relation to security, preparedness and response shall be defined and approved by management, published and communicated to employees, and implemented across organisation	For example: • Access Control • Incident Response (lockdown, evacuation invacuation) • Suspicious behaviour reporting • CCTV etc.

A.5	**Active**	**Review of security, preparedness and response related procedures and plans**	All procedures and plans relating to security, preparedness and response shall be reviewed at planned intervals, or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Consider: • Annual review / periodic review • Review following: change to threat landscape, increase in vulnerabilities, resourcing, or assets
B. INTERNAL ORGANISATION				
Objective: to establish a framework to initiate and control the implementation and operation of security related matters within the business.				
No.	**Type**	**Control**	**Description**	**Considerations**
B.1.	**Active**	**Roles and responsibilities**	All preparedness, security and response related responsibilities shall be defined, allocated and communicated to all employees. Employees shall be kept up to date of any changes to roles and responsibilities.	Consider: • A responsible person to take ownership of counter-terrorism risks • A competent person to advise on counter-terrorism related risks and validate control measures • Roles and responsibilities allocated via policies and procedures or role profiles (e.g. patrolling, first aid, CCTV etc.)
B.2.	**Active**	**Segregation of duties**	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for exploitation and misuse of business assets.	For example: • Role-based access control (e.g. permissions and privileges assigned to specific roles rather than individual users).
B.3.	**Active**	**Collaborative arrangements with authorities and wider support network**	Collaborative arrangements shall be established and maintained with other organisations in your support network in relation to security incidents.	Consider: • Co-ordinated response plans with neighbouring businesses and emergency services • Collaborative testing and exercising etc.
C. PEOPLE AND PERSONNEL				
Objective: to ensure that employees and contractors understand their roles and responsibilities and are suitable for the roles for which they are considered				
No.	**Type**	**Control**	**Description**	**Considerations**

C.1.	**Active**	**Management responsibilities (people and personnel)**	Management shall require all employees and contractors to be aware of existing security, preparedness and response measures in accordance with the established policies and procedures of the business. Any changes to security, preparedness and response policies and procedures should be communicated to all employees as and when these changes occur.	Consider: • CT Training and guidance, including refresher training • Staff briefings / threat briefings, including updates and changes
C.2.	**Active**	**Pre-employment screening**	Document verification shall be undertaken on all candidates considered for employment in accordance with relevant laws, regulations and ethics. These shall be proportional to business requirements, the level of access required, and the perceived risks.	Consider: • Basic identity, financial, employment and criminal record checks • Social media checks • British Standard 7858 (or equivalent) for security screening of employees
C.3.	**Active**	**Document awareness**	Document awareness training shall be undertaken by staff members responsible for verifying document, with consideration for document verification equipment to assist in this process.	Consider: • Training and guidance (e.g. spotting forgery and counterfeits) for employees responsible for screening and pre-employment checks • Magnifiers and UV lights to help detect fraudulent documentation.
C.4.	**Active**	**Counter-terrorism training and awareness**	All employees and, where relevant, contractors shall receive appropriate security and CT awareness education and training. Regular updates should be provided in accordance with established policies and procedures of the business.	Consider: • ACT e-Learning and SCaN for all staff for new staff as part of induction packages • Refresher training • Maintaining records of staff training completion
C.5.	**Active**	**Incident response training and awareness**	All staff and, where relevant, contractors shall receive appropriate incident response training and guidance. Regular updates should be provided in accordance with established policies and procedures of the business.	Consider: • Delivering training on response procedures as part of your staff induction packages and staff refresher training
D.	**ACCESS CONTROL**			

Objective: to limit access to restricted areas, systems and applications to authorised individuals only.				
No.	**Type**	**Control**	**Description**	**Considerations**
D.1.	**Active**	**Access control policy**	An access control policy shall be established, documented and reviewed based on business and security requirements. This shall specify how access is managed, who may have access to specific areas, systems and applications, and under what circumstances	Consider: • Objectives and scope • Roles and responsibilities • Related policies • Policy statements (e.g. user access rights management, physical access and controls etc.) • Compliance
D.2.	**Active**	**Management of access rights**	The allocation and use of access rights shall be restricted and controlled (electronic access, application and systems access and / or key holders)	For example: • Key holders restricted to management with opening or closing responsibilities
D.3.	**Active**	**Review of user access rights**	Users' access rights shall be reviewed at regular intervals.	For example: • Review system and application access every six months; change mechanical PIN code locks regularly.
D.4.	**Active**	**Removal or adjustment of access rights**	The access rights of all employees and external party users to the premises shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	For example: • System and application access removed and mechanical PINs changed upon staff leaving.
SYSTEM AND APPLICATION ACCESS CONTROL				
No.	**Type**	**Control**	**Description**	**Considerations**
D.5.	**Active**	**User access control policy**	A user access control policy (system and application access) shall be established, documented and reviewed based on business and security requirements. This shall specify how user accounts and privileges are created, managed and deleted	For example: • Objectives and scope • Roles and responsibilities • Related policies • Policy statements (e.g. principle of least privilege, password control management, user access account management etc. • Compliance

D.6.	**Active**	**Information access restriction**	Access to information and application system functions shall be restricted in accordance with the access control policy.	For example: • Limit user execution permissions • Enforce the principle of least privilege
D.7.	**Active**	**Secure log-on procedures**	Where required by the access control policy, access to systems applications shall be controlled by a secure log-on procedure.	For example: • Password protection for all business issued desktops, laptops, smartphones and tablets • Drive encryption keys
STAFF & VISITOR PASSES				
No.	**Type**	**Control**	**Description**	**Considerations**
D.8.	**Active**	**Staff and visitor pass procedure**	A staff and visitor pass procedure shall be established, documented and reviewed based on business and security requirements.	Consider: • Issuing and pass discipline • Lost and stolen passes • Visitor supervision requirements and logs • Notice times and visit times
D.9.	**Active**	**Staff and visitor passes**	All staff, contractors and visitors shall prominently display a valid pass at all times on site.	For example: • Photographic pass cards for all employees / contractors • Temporary passes for visitors following verification checks
E.	**PHYSICAL ENVIRONMENT SECURITY**			
Objective: to prevent unauthorised physical access, damage and interference				
No.	**Type**	**Control**	**Description**	**Considerations**
E.1.	**Active**	**Physical security policies**	A physical security policy (or set of policies) shall be established, documented and reviewed based on business and security requirements	Consider: • Objectives and scope • Role and responsibilities • Related policies • Policy statements (e.g. physical entry controls, search and screening, CCTV etc.)
E.2.	**Physical**	**Perimeter security**	Security perimeters shall be defined and used to protect areas restricted / secure areas.	For example: • Fencing

				• Intrusion detection systems • Movement-based lighting • Airspace restrictions, geo-fencing etc.
E.3.	**Physical**	**Physical entry controls**	Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	For example: • Swipe access control doors • Mechanical PIN locks.
E.4.	**Physical**	**Securing offices, rooms and facilities**	Physical security for offices, rooms and facilities shall be designed and applied.	For example: • Lockable windows, doors, grilles etc.
E.5.	**Physical**	**Working in secure areas**	Procedure for working in secure areas shall be designed and applied.	Consider: • Access control requirements • Dedicated air handling facilities • Specifications for walls, windows and doors etc.
E.6.	**Physical**	**Delivery and loading areas**	Delivery and loading areas, and other points where unauthorised persons could enter the premises, shall be controlled to avoid authorised access.	For example: • Swipe card access to secure areas and loading bays
E.7.	**Physical**	**Parking areas**	Parking areas, and other points where unauthorised persons could enter the premises, shall be controlled to avoid unauthorised access.	For example: • Limit and control vehicle access through access control points.
E.8.	**Physical**	**Vehicle security barriers**	Vehicle security barriers (VSBs) shall be installed to provide protection from hostile vehicles.	For example: • Bollards gates, ditches • Streetscape products (e.g. planters, benches)
E.9.	**Physical**	**Traffic calming measures**	Traffic calming measures shall be implemented to limit vehicle approach speeds to a manageable level.	For example: • Road humps, speed limits, speed cushions, lane width restrictions
E.10.	**Physical**	**Search and screening**	A search and screening procedure shall be defined and implemented in line with security requirements.	Consider: • Post and delivery screening • Identity checks for all personnel and vehicles (including emergency services)

				• Appropriate techniques for staff searches in publicly accessible location • Personnel, bag and vehicles searches.
E.11.	**Active**	**CCTV and video surveillance policy**	CCTV shall be defined in line with security requirements. This shall be captured in a dedicated CCTV policy	Consider: • Scope and objectives • Roles and responsibilities • Related policies • Policy statements • Operational statements (e.g. camera locations and details) • Storage and retention methods • Compliance
E.12.	**Physical**	**CCTV and video surveillance**	CCTV shall be implemented in line with security requirements and the CCTV video surveillance policy.	For example: • Passive CCTV (recording only) • Intelligent CCTV
E.13.	**Active**	**Review of CCTV and video surveillance**	CCTV procedures shall be reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness	Consider: • Review of CCTV procedures following a change in threat level • Periodic review
E.13.	**Active**	**Physical security training**	Physical security measures will be underpinned by appropriate training and exercising.	For example: • Practical scenario training • Face-to-face training and briefings • Online training (e.g. search training; SCaN for CCTV operators)
E.14.	**Active**	**Security patrol strategy**	A security patrol strategy and procedure shall be defined and implemented in line with security requirements.	Consider: • Scope and objectives • Staff and management • Roles and responsibilities • Related policies • Patrolling strategy (internal and external areas)

E.15.	**Physical**	**Security patrols**	Security patrols shall be implemented in line with security requirements and the security patrol strategy.	Consider: • Internal / external guarding team • Periodic staff perimeter and building checks.
F.	**CYBERSECURITY**			
Objective: to ensure the protection and security of information generate, stored or transferred by an organisation				
No.	**Type**	**Control**	**Description**	**Considerations**
F.1.	**Active**	**Policies for cyber and information security**	A policy (or set of policies) in relation to cyber and information security shall be defined and approved by management, published and communicated to employees and any relevant external parties	Consider: • Scope and objectives • Roles and responsibilities • Related policies • Policy statements (e.g. network controls, patch management, information transfer etc.)
F.2.	**Physical**	**Controls against malware**	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	For example: • Anti-malware software • Awareness training for all staff
F.3.	**Physical**	**Network controls**	Networks shall be managed and controlled to protect information in systems and applications	For example: • Boundary firewalls and internet gateways • Network perimeter defences (e.g. web proxy, web filtering, content checking etc.)
F.4.	**Physical**	**Password management system**	Password management system shall be interactive and shall ensure quality passwords	Consider: • Encryption for all passwords • Multi-factor authentication
F.5.	**Physical**	**Patch management**	Identified technical vulnerabilities will be identified in a timely fashion to limit exposure and address the associated risk.	Consider: • Software and firmware updates
F.6.	**Physical**	**Listing and execution control**	Unknown software and devices shall be prevented from running or installing.	For example: • Auto-run on USB and CD drives disabled • Cryptographic controls

F.7.	**Physical**	**Secure configuration**	The functionality of all business devices shall be restricted to the minimum required for business to function	For example: • Group policy to set security policy • Site database permissions • Access control lists (ACLs)
F.8.	**Physical**	**Information transfer**	Procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Consider: • Email Usage • Media Handling • Information Sharing Agreements (ISA)
F.9.	**Physical**	**Clear desk and screen**	A clear desk and screen procedure shall be adopted for all desktops, laptops, tablets etc.	For example: • Screen timeout applied to all laptops, tablets, desktops • Removable storage media and records kept in locked drawers or cabinets when not in use
G.	**ASSET SECURITY**			
Objective: to prevent loss, damage, theft or compromise of organisational assets				
No.	**Type**	**Control**	**Description**	**Considerations**
G.1.	**Physical**	**Asset siting and protection**	Organisational assets shall be sited and protected to reduce opportunities for unauthorised access and interference.	For example: • CCTV covering all communal areas and vulnerable points • Equipment kept in secure locations with access control (e.g. controlled access for server rooms)
G.2.	**Physical**	**Removal of assets**	Organisational assets shall not be taken off-site without prior authorisation.	For example: • Devices and equipment kept securely on premises unless authorised by management for off-site use
G.3.	**Physical**	**Security of assets off-premises**	Security shall be applied to off-site assets taking into account the different risks of working outside the business premises.	For example: • Disk encryption for laptops to complement normal user logins.
H.	**SERVICE DELIVERY AND HOUSEKEEPING**			

Objective: to reduce opportunities for interference and help manage false alarms and hoaxes.				
No.	**Type**	**Control**	**Description**	**Considerations**
H.1.	**Physical**	**Waste disposal management**	The security of all waste disposal methods (e.g. litter bins, skips, compactors etc.) shall be considered as part of waste disposal management and reviewed in line with security management policies and procedures.	Consider: • Management and placement of all litter bins • Clear bags for waste disposal
H.2.	**Physical**	**Supply chain management**	The security of supply chains shall be reviewed in line with security management policies and procedures.	Consider: • Food and Drink Defence (PAS 96:2017) • Controlled access for all persons and vehicles • Secure storage for transport vehicles and on-site materials
H.3.	**Physical**	**Estate management**	The security of the estate grounds and buildings shall be considered as part of estates management and reviewed in line with security management policies and procedures.	For example: • Public, communal and external areas kept clean, tidy and well lit; • Trees and vegetation pruned to assist CCTV and natural surveillance.
H.4.	**Physical**	**Utility management**	The security of air-handling systems, water tanks and other key utilities shall be reviewed in line with security management policies and procedures.	For example: • Restrict access to water tanks and other key utilities • Improve air-filters or upgrade HVAC systems as necessary.
H.5.	**Physical**	**Equipment management**	The provision and security of all equipment shall be considered as part of equipment management and reviewed in line with security management policies and procedures.	Consider: • PAT testing • Equipment maintenance schedule • CCTV equipment servicing • Fire extinguishers and first aid kits.
I. COMMUNICATIONS				
Objective: to ensure adequate internal and external communications are established and maintained.				
No.	**Type**	**Control**	**Description**	**Considerations**

I.1.	**Active**	**Communications policy**	A communications policy (or set of policies) shall be established, documented and reviewed based on business and security requirements	Consider: • Scope and objectives • Roles and responsibilities • Related policies • Policy statements (e.g. strategy, internal communications, external communications, crisis communications for security incidents)
I.2.	**Active**	**Security-minded communications strategy**	A communications strategy shall be adopted by the organisation that audits and adapts information for the purpose of protective security. The security capability of the organisation shall also be amplified across a range of communication channels to assist with deterrence.	For example: • Audit the organisation's digital footprint to identify information that may assist and motivate attack planning • Adapt or remove information that increases vulnerabilities • Amplify proactive marketing of security capabilities across a range of communication channels.
I.3.	**Active**	**Internal communications**	Internal communications shall be defined and established through relevant procedures and protocols.	Consider: • Reporting procedure for security incidents • Crisis Communications Plan with up to date contact lists for key team members • Staff training and guidance on reporting suspicious activity.
I.4.	**Active**	**External communications**	Communication links shall be established with authorities and wider support network to share information relating to suspicious activity and security incidents, and co-ordinate security incident plans.	For example: • Communication links with neighbouring businesses established and maintained (e.g. up to date contact lists and details) • Communication links established with local police force
J.	**SECURITY INCIDENT PREPAREDNESS AND RESPONSE**			
Objective: to ensure adequate preparations have been made to effectively respond to a security incident				

No.	Type	Control	Description	Considerations
J.1.	**Active**	**Move to Critical (MTC) plan**	A Move to Critical (MTC) plan shall be established to respond to an increase in threat level or a terrorist incident.	Consider: • National Stakeholder Menu of Tactical Options (MoTO)
J.3.	**Active**	**Reporting procedure**	Management responsibilities and procedures shall be established for reporting and escalating security incidents.	Consider: • Staff and management roles and responsibilities • Escalation criteria and routes; • Communication plans with neighbouring businesses and emergency services • Guidance and briefings for all staff on challenging and reporting • Reporting logs
J.4.	**Active**	**Crisis communication plan**	A crisis communication plan shall be established to guide action and communication during a security incident.	Consider: • Staff and management roles and responsibilities • Communication with neighbouring businesses and emergency services; a selection of responses suitable for a range of security incidents (e.g. VAW, MTA etc.)
J.5.	**Active**	**Suspicious behaviour response procedure**	Management responsibilities and procedures shall be established for suspicious behaviour.	Consider: • Identification of applicable protocols (e.g. Deny, Detect, Deter, SCaN) • Reporting and escalation procedure • Staff and management roles and responsibilities • Communication plans (internal and external).
J.6.	**Active**	**Suspicious items response procedure**	Management responsibilities and procedures shall be established for suspicious items	Consider: • Identification of applicable protocols (e.g. HOT protocol, 4 Cs) • Reporting and escalation procedure

				• Staff and management roles and responsibilities • Communication plans (internal and external).
J.7.	**Active**	**Lockdown, invacuation and evacuation response procedure**	Lockdown, invacuation and evacuation plans and procedures shall be established which designate route and rendezvous points and outlines management / staff roles and responsibilities, including individual evacuation plans for disabled staff. All staff and visitors should be briefed on these procedures.	Consider: • Identification of invacuation, evacuation and rendezvous points and routes • Staff and management roles and responsibilities • Dedicated plans for disabled staff • Co-ordination plans with neighbouring businesses and emergency services • Communication plans (internal and external)
J.8.	**Active**	**Bomb threat procedures**	A bomb threat procedure shall be established in line with security management policy and communicated to all staff, contractors and visitors.	Consider: • Identification of applicable protocols (e.g. 4Cs protocol, ETHANE) • Bomb Threat Checklist • Incident response plans (e.g. lockdown, evacuation and invacuation) • Co-ordination plans with neighbouring businesses and emergency services • Communication plans (internal and external)
J.9.	**Active**	**MTA response procedures**	A MTA plan and procedure shall be established in line with security management policies and communicated to all staff, contractors and visitors.	Consider: • Identification of applicable protocols (e.g. RUN HIDE TELL, ETHANE) • Reporting and escalation procedure • Incident response plans (e.g. lockdown, evacuation, invacuation) • Communication plans (internal and external)

J.10.	**Active**	**C-UAS response procedures**	A countering threats from Unmanned Aerial Systems (C-UAS) plan and procedure shall be established in line with security management policies and communicated to all staff, contractors and visitors.	Consider: • Reporting and escalation procedure • Incident response plan for sightings and confirmed presence • Staff and management responsibilities • Co-ordination with neighbouring businesses and emergency services • Communications plans (internal and external)
J.11.	**Active**	**CBRN response procedures**	A CBRN response plan and procedure shall be established in line with security management policies and communicated to all staff, contractors and visitors.	Consider: • Reporting and escalation procedure • identification of applicable protocols (e.g. Remove, Remove, Remove protocol, ETHANE) • incident response plans (e.g. evacuation, invacuation, lockdown) • HVAC emergency shut-down procedure • Staff and management responsibilities • Communication plans (internal and external)
J.12.	**Active**	**CCTV response procedure**	A CCTV response plan and procedure shall be established in line with security management policy.	Consider: • Reporting and escalation procedure • Identification of applicable protocols (e.g. ETHANE) • identification of vulnerable points and routes (e.g. entry points, stairwells) • Staff and management responsibilities • Attack monitoring • Communication plans (internal and external)

J.13.	**Active**	**Vehicle as a weapon plans and procedures**	A VAW response plan and procedure shall be established in line with security management policy.	Consider: • Reporting and escalation procedure • Identification of applicable protocols (e.g. RUN HIDE TELL) • Incident response plans (e.g. lockdown, evauaction, invacuation) • Communication with neighbouring businesses and emergency services(e.g. internal and external); • Staff and management responsibilities
J.14.	**Active**	**Cyber-attack plans and procedures**	A cyber-attack plan and procedure shall be established in line with security management policy.	Consider: • Staff and management roles and responsibilities • Reporting and escalation procedure • Technical response capabilities; • Playbooks (e.g. malware infection response plan, data breach response plan) • communication plans (e.g. internal and external)
J.15.	**Active**	**Fire as weapon plans and procedures**	A fire as weapon plan and procedure shall be established in line with security management policy.	Consider: • Reporting and escalation procedure • Identification of existing fire safety measures • Incident response plans (e.g. evacuation) • Communication with neighbouring businesses and emergency (e.g. internal and external) • Staff and management responsibilities • Co-ordination plans with neighbouring businesses

J.16.	**Active**	**First aid response plans and procedures**	A first aid response plan and procedure shall be established in line with security management policy.	Consider: • Needs assessment (consider circumstances of your workplace, workforce and hazards and risks) • Strategic oversight • Management and direction setting for administration of first aid • Provisions and training (including awareness for non-employees)
J.17.	**Active**	**Incident response testing and exercising**	Security incident response procedures and protocols shall be tried and tested at regular intervals to ensure their continuing suitability, adequacy and effectiveness.	For example: • Table-top exercises • Live exercises • Discussion-based exercises
J.18.	**Physical**	**Incident response equipment**	Equipment required during an emergency responses shall be sourced, maintained and prepositioned for use during a security incident.	For example: • First aid kit • Eyewash and flushing kit • PaCT kits • Fire extinguishers • Defibrillators • Grab bags
K.	**SECURITY INCIDENT MANAGEMENT**			
Objective: to ensure a consistent and effective approach to the management of security incidents, including communication on security incidents and weaknesses				
No.	**Type**	**Control**	**Description**	**Considerations**
K.1	**Active**	**Incident Management Plan (IMP)**	An Incident Management Plan (IMP) shall be established to manage a security incident from occurrence to business recovery	Consider: • Procedures and plans • Roles and responsibilities • Incident room details • Key locations
K.2.	**Active**	**Response to security incidents**	All security incidents shall be responded to in accordance with documented procedures.	For example: • Reporting and escalation procedures

				• Response and incidents plans and procedures
K.3.	**Active**	**Management of security incidents**	All security incidents shall be managed in accordance with documented procedures.	For example: • Incident response procedure and plans (e.g. MTA; VAW; Cyber)
K.4.	**Active**	**Learning from security incidents**	Knowledge gained from analysing and resolving security incidents shall be used to reduce the likelihood or impact of future incidents	Consider: • Post incident reviews • Risk reviews and monitoring
K.5.	**Active**	**Collection of evidence**	The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information relating to security incidents which can serve as evidence.	For example: • Evidence capture and collection embedded into security incident response plans and procedures.
L.	**BUSINESS CONTINUITY**			
Objective: business continuity arrangements shall be developed and embedded to maintain critical and urgent business activities				
No.	**Type**	**Control**	**Description**	**Considerations**
L.1.	**Active**	**Business continuity plan**	The organisation shall determine the scope, requirements and management responsibilities for business continuity in the event of a terrorist attack. This should be outlined in a plan (or policy) that shall be defined and approved by management, and published and communicated to all relevant parties.	Consider: • Aims and objectives • Governance and responsibilities • Essential processes • Staff details and key contacts • Immediate and response actions • Post-incident resources and equipment • ISO 22301 Societal Business Management Security Systems and Guidance • Business Continuity Institute (BCI) GPG (Good Practice Guidelines)
L.2.	**Active**	**Review business continuity plan**	The organisation shall verify the established and implemented business continuity measures at regular intervals in order to ensure that they are valid and effective during emergency situations.	Consider: • Annual review • Review following change to threat landscape or incident

				• Review following change in resourcing
L.3.	**Active**	**Business continuity procedures**	The organisation shall establish, document and implement procedures to ensure the required level of business continuity.	Consider: • Buildings • People (colleagues and suppliers) • Equipment (machinery and IT)